



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/642,879	08/21/2000	Stephen Michael Matyas JR.	5577-208	8114

20792 7590 01/14/2005

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER

TRAN, ELLEN C

ART UNIT PAPER NUMBER

2134

DATE MAILED: 01/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/642,879

Applicant(s)

MATYAS ET AL.

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 July 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-66 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1-28 is/are allowed.
- 6) ☒ Claim(s) 29-66 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input checked="" type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>Jul'04 & Sep'04</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is responsive to communication: 15 July 2004, the amendment to the specification and claims is accepted.
2. Claims 1-66 are currently pending in this application. Claims 1, 17, 29, 41, 53, 65, and 66 are independent claims.

Response to Arguments

3. Applicant's arguments with respect to claims 29-66 have been considered but are not persuasive.

In response to argument starting on page 31, line 7, "Applicants submit that Claim 29 is neither disclosed nor suggested by the cited portions of Narasimhalu ... Thus Claim 29 also provides for three encryption keys. As discussed above, Narasimhalu describes the use of two keys, not three". The office disagrees, although claim 17 is considered allowable because the references uses only two key versus three. The claimed invention in claim 29 does not contain allowable subject matter because it is directed to a program that encrypts per request there is no distinction for the use of three keys.

In response to argument starting on page 32, line 30 "Claims 41, 53, 65, and 66 are system and computer program product claims corresponding to Claims 17 and 29". The office disagrees that these claims are allowable because the claimed invention could be exercised in a program only and the text in the claims has no effect on the processor.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 29, 31-44, 48-53, 55-66 are rejected under 35 U.S.C. 102(b) as being anticipated by Narasimhalu et al. U.S. Patent No. 5,499,298 (hereinafter '298).

As to dependent claim 29, **“A method for controlling access to digital data of a file in a file system having a personal key server”** is taught in '298 col. 5, lines 4-15;

“the personal key server carrying out the steps of receiving a request from a requester to create a file header associated with the file, the request containing an encryption key encrypted with a personal key” is shown in '298 col. 6, lines 1-15;

“encrypting the encrypted encryption key with a control key to provide the file header containing an encryption key encrypted with both a personal key and a control key; and returning the file header to the requestor” is disclosed in '298 col. 5, lines 35-47.

As to dependent claims 31, **“further comprising: receiving a request from the personal key client to recover the encrypted encryption key containing the encryption key encrypted with the personal key and the control key; decrypting the encryption key encrypted with the personal key and the control key with the control key; returning the encryption key encrypted with the personal key”** is taught in '298 col. 5, lines 35-47.

As to dependent claim 32, **“further comprising: receiving a request to update the file header to incorporate an encryption key encrypted with a new encryption key; encrypting**

Art Unit: 2134

the encryption key encrypted with the new encryption key with the control key to provide a control key encrypted new encryption key encrypted encryption key; incorporating the control key encrypted new encryption key encrypted encryption key in the file header to provide an updated file header; and returning the updated file header” is taught in ‘298 col. 10, lines 32-46.

As to dependent claim 33, “wherein the request to update of the file header to incorporate the encryption key encrypted with a new encryption key includes an identification of a user requesting to update the file header, the method further comprising: comparing the identification of the user requesting to update the file header with a list of users authorized to access the file; and rejecting the request if the user requesting to update the file header is not identified in the list of users authorized to access the file as the owner of the file” is shown in ‘298 col. 10, lines 32-46 (i.e. “identification of a user” same as “CID”).

As to dependent claim 34, “wherein the request from a requestor to create a file header associated with the file, further contains an unencrypted encryption key associated with users authorized to access the file, the method further comprising: encrypting the unencrypted encryption key with the control key; incorporating the unencrypted encryption key encrypted with the control key in the file header; and returning the file header incorporating the encryption key encrypted with the control key” is disclosed in ‘298 col. 6, lines 41-43 (i.e. “unencrypted encryption key” same as “public key DPK”)

As to dependent claim 35, further comprising: receiving a request to recover the encryption key in response to a request by a user other than an owner of the file continuing

the encryption key encrypted with the control key; decrypting the encryption key encrypted with the control key with the control key; and returning the encryption key” is taught in ‘298 col. 10, lines 11-28.

As to dependent claim 36, “wherein the request to recover the encryption key includes an identification of the user requesting to access the file, the method further comprising: comparing the identification of the user requesting to access the file with a list of users authorized to access the file; and rejecting the request if the user requesting to access the file is not identified in the list of users authorized to access the file” is taught in ‘298 col. 11, lines 1-30.

As to dependent claim 37, “wherein the request to create a file header associated with the file includes a public key encrypted encryption key corresponding to each user authorized to access the file other than an owner of the file and a list containing each user authorized to have access to the file, the method further comprising: encrypting each public key encrypted encryption key with the control key; incorporating each public key encrypted encryption key encrypted with the control key in the file header; returning the file header incorporating each public key encrypted encryption key encrypted with the control key” is shown in ‘298 col. 11, lines 1-11.

As to dependent claim 38, “further comprising the step of creating an access control list from the list provided with the request” is disclosed in ‘298 col. 11 lines 13-30 (i.e. “access control list” same as “one of the AWs found in field 142”).

As to dependent claim 39, “further comprising: receiving a request to recover the public key encrypted encryption key containing the public key encrypted encryption key

encrypted with the control key corresponding to a user requesting access to the file;
decrypting the public key encrypted encryption key encrypted the control key with the
control key; and returning the public key encrypted encryption key corresponding to the
user requesting the file” is taught in ‘298 col. 6, lines 1-12.

As to dependent claim 40, “further comprising: comparing the identification of the
user requesting to access the file with the list of users authorized to access the file; and
rejecting the request if the user requesting to access the file is not identified in the list of
users authorized to access the file” is taught in ‘298 col. 11, lines 1-30.

As to independent claim 1, this claim is directed to the system of claim 29 and is
rejected along similar rationale.

As to independent claim 41, this claim is directed to a personal key client for the system
of method of 29 and is rejected along the same rational.

As to dependent claims 42-44 and 48-52, these claims incorporate substantially similar
subject matter as above claims 30-40 above and are rejected along the same rationale.

As to independent claim 53, this claim is directed to a personal key server system of the
method of claim 29 and is rejected along the same rationale.

As to dependent claims 55-64, these claims incorporate substantially similar subject
matter as claims 30-40 and are rejected along the same rationale.

As to independent claim 65, this claim is directed to a computer program product of the
method of claim 29 and is rejected along the same rationale.

As to independent claim 66, this claim is directed to a computer program product of the
method of claim 29 and is rejected along the same rationale.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 45-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘298 in further view of Carroll U.S. Patent No. 6,105,131 (hereinafter ‘131).

As to dependent claim 45, **“to provide a new file header; and storing the new file header at the file server”** is taught in ‘298 col. 6, lines 27-32 “Although PKC is referred in the embodiment of the present invention, any method of encryption is applicable. Next a medium signature 36 is created from the particular distribution medium on which COIN is encrypted with K1. It follows that the body 40 of the sealed COIN is generated. In step 68, the header is prepared next”;

the following is not taught in ‘298:

“further comprising: encrypting the encryption key with a public key of a trusted third party; incorporating the encryption key encrypted with the public key of a trusted third party into the received file header” however ‘131 teaches “A certificate (also called digital certificate) is an electronic credential issued by a trusted third party ... Encryption certificates provide certification of encryption keys used” in col. 4, lines 46-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for controlling access to digital data of a file taught in ‘298 to include a means to issue keys by a trusted third party. One of ordinary skill in the art would have been

Art Unit: 2134

motivated to perform such a modification to enhance security see '131 (col. 1, lines 29 et seq.)

"Some web browsers provide a secured link by utilizing a security protocol, ... However, these safe guards fail to provide enough security".

As to dependent claim 46, **"further comprising: receiving a request"** is taught in '298 col. 11, line 1 "with an information consumer making an access request";

"by the trusted third party to access the file; requesting access to the file by the trusted third party from the file server; receiving the encrypted file and the file header from the file server" is taught in '131 col. 4, lines 9-13 "The computer network 14 connects user terminals 18 and RA terminal 16 to secure server 12 and third party terminals 66".

"extracting the encryption key encrypted with the public key of the trusted third party from the received file header; obtaining the private key of the trusted third party; decrypting the extracted encryption key encrypted with the public key of the trusted third party to recover the encryption key; and decrypting the encrypted file with the recovered encryption key" is disclosed in '298 col. 7, lines 60-67 "the controller extracts in step 95 the encryption/decryption key".

As to dependent claim 47, **"further comprising: requesting the file header associated with the file from the file server; receiving the file header from the file server"** is taught in '298 col. 11, lines 1-11 "with an information consumer making an access request ... the information provider finds the corresponding key K_H , which it used in step 156 to encrypts the header fields 119";

"extracting the encryption key encrypted with the personal key and the control key; requesting recovery of the encrypted encryption key; receiving the recovered encrypted

encryption key; generating the personal key; decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key” is shown in ‘298 col. 7, lines 60-67 “the controller extracts in step 95 the encryption/decryption key $K_{TAL-LAL+1}$ from the header 35. The Controller 45”;

“obtaining a new public key associated with the trusted third party” is disclosed in ‘131 col. 4, lines 46-67 “A certificate (also called ditgital certificate) is an electronic credential issued by a trusted third party ... Encryption certificates provide certification of encryption keys”;

“encrypting the recovered encryption key with the new public key to provide a new public key encrypted encryption key; incorporating the new public key encryption key in the file header to provide an updated file header; and providing the updated file header to the file server” is taught in ‘298 col. 10, lines 47-65 “The information provider is ready to generate a Sealed-COIN in step 150 if it has CID and the values of the associated ... The header fields 119 in turn are encrypted in step 156 to form the header with a new key K_H ”.

8. **Claims 30 and 55** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘298 in further view of Howard et al. U.S. Patent No. 6,678,731 (hereinafter ‘731).

As to dependent claim 30, and rejecting the request if the authentication ticket is invalid” is disclosed in ‘298 col. 11, lines 13-30 “If any of these checks fail, access to controlled information is denied”;

the following is not taught in ‘298:

“wherein the request further includes an authentication ticket, the method further comprising the steps of: determining the validity of the authentication ticket however ‘731

teaches “a request from a network server to authenticate a user who is seeking access ... The process determines whether the user was already authenticated by the authentication server” in col. 2, lines 44-55.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for controlling access to digital data of a file taught in ‘298 to include a means to utilize an authentication server. One of ordinary skill in the art would have been motivated to perform such a modification to make information more easily available to valid users see ‘731 (col. 1, lines 50 et seq.) “If a user visits several different web sites, each web site may require entry of similar registration information about the user ... This repeated entry of identical data is tedious when visiting multiple web sites in a short period of time”.

As to dependent claim 54, this claim contains substantially similar subject matter as cited in the above claim 30 and is rejected along the same rationale.

Allowable Subject Matter

9. The following is an examiner’s statement of reasons for allowance: Claims 1-28 are allowed, in view of arguments presented in amendment starting on page 30 line 25, that the reference describes a system that uses only two keys whereas the invention utilizes three encryption keys.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not

Art Unit: 2134


mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
04 January 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100